STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

INFORMATION WARFARE: IMPACTS ON COMMAND AND CONTROL DECISION-MAKING

BY

LIEUTENANT COLONEL(P) ROBERT E. JOHNSON
United States Army

USAWC CLASS OF 1996

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

UNCLASSIFIED

USAWC STRATEGY RESEARCH PROJECT

INFORMATION WARFARE: IMPACTS ON COMMAND AND CONTROL DECISION-MAKING

by

Lieutenant Colonel(P) Robert E. Johnson
United States Army

Colonel(Ret) Arthur J. Lykke
Project Adviser

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Robert E. Johnson, LTC(P), USA

TITLE: Information Warfare: Impact on Command and Control Decision-Making

FORMAT: Strategy Research Project

DATE: 15 April 1996 PAGES: 28 CLASSIFICATION: Unclassified

The military's senior leadership has openly acknowledged that in future wars we must win the information war to achieve decisive victory. This paper reviews decision--making when command and control (C2) systems are interrupted, contaminated, or destroyed. The United States is an information dominant society. For every technological advancement in the development of an offensive information-based system, our vulnerability to information warfare increases. Future conflicts will undoubtedly include threats to degrade our information systems. Are we training our leaders to respond in an environment where our information systems are corrupted, manipulated, or destroyed? As we prepare to "Win the Information War," our leaders must not allow predictable attacks on their information--based technology to force them toward unfavorable conflict resolution. "Winning the Information War" must include contingency planning for disruptions in the flow of information.

INTRODUCTION

Clearly, winning the information war has become a key element of the services national military strategy. But, knowledge based warfare is not new. Sun Tzu said, "Know the enemy and know yourself; in a hundred battles you will never be in peril. When you are ignorant of the enemy and know yourself, your chances of winning and losing are equal. If ignorant both of your enemy and yourself, you are certain in every battle to be in peril." From Sun Tzu's time through the beginning of the Civil War, transfer of information was an important factor in commanders' attempts to make rapid and accurate decisions, but availability of such information was quite limited. During the Civil War the telegraph was first used tactically in June 1861 to direct fire of batteries on Fort Calhoun against the Confederate positions at Sewell's Point opposite Fort Monroe. The first permanent line of communication using semaphores and lights was set up between Newport News and Fort Monroe, establishing the standards and system procedures for the U.S. Army. By the end of the war, the War Department had strung more than 15,000 miles of cable and transmitted about 3,330 messages a day on the system[1].

This introduction of information technology has forever altered the course of war. The telegraph and subsequent developments enabled commanders thousands of miles away to maintain an electronic battlefield presence and eventually to coordinate theater--wide operations. In World War II,

development of radar, advances in radio communication, the beginnings of cybernetics and the deciphering of intercepted German (Ultra) and Japanese (Magic) messages were incredible, creative, innovative accomplishments in the paradigm shift toward information warfare[2].

Thus over the past 150 years information technology has increased in complexity and become indispensable to combat operations. Modern militaries are utterly dependent upon information technology to maintain, deploy, and employ virtually every weapon system in their arsenals.

Today the battle cry of our military senior leaders is that we must win the information war. Major General Paul Funk, former Commander, U.S. Army Armor School, declared, "If this is the information age, then by God we have to win the information war." The information age has thrust us into a new paradigm. It is no longer business as usual; we must posture ourselves for the offensive and defensive implications of information--based warfare. If information war is to serve as a genuine combat multiplier, we must anticipate the impacts on decision--making if a potential adversary successfully degrades, destroys, or corrupts some portion of our information--based systems.

WINNING THE INFORMATION WAR

General Sullivan, former Chief of Staff of the Army, asserted, "We must, above all, win the information war." Winning the information war is not simply about intelligence, nor is it about data transmission. It is about taking the information that is available to any given soldier and making it available to whoever needs it[3].

In a combat environment, winning the information war through rapid exchange of information horizontially and vertically will enable battle commanders, fire supporters, logisticians, and transporters to share a common, real--time situational awareness. This capability will allow us to apply power to the main effort quickly, to attack the enemy simultaneously throughout the battle area, and to do it over and over again. The enemy will have no time to react, recover, or regroup[4].

In an earlier era, to meet World War II's challenges, the National Defense Research Council had overall responsibility for technological research and systems development. In early May 1944, a team of scientists from Division 15 went to England in preparation for the Allied invasion of Europe. They provided technical advice and assistance in the "electron war."

The Operation Overlord invasion of France on 6 June 1944 offers a classic study of the role of information warfare in a large, complex campaign. Overlord relied upon detailed deception planning (Bodyguard), which included giving the Germans false

clues that an invasion would occur in Norway (Fortitude North), at the Pas de Calais in France (Fortitude South), in Greece, Italy, and at the Bay of Biscay along the French Coast[5].

To ensure the Germans received the deceptive messages, the Allies relied on Ultra intelligence to read German communication. Messages from the Germans' most trusted agents-their spies in the United Kingdom-were all written by the Allies. In preparation for the invasion, a joint U.S. and British Radio Countermeasures Committee was set up. Their mission was to protect Allied signal frequencies while jamming and deceiving German radar and disrupting their communications from Luftwaffe fighters that could find, disrupt, and destroy the Allied Naval flotilla crossing the English Channel. They used British naval and air jammers such as Ground Cigar, Aspirin, Grover, and Tuba. These information warfare devices deceived both Field Marshals Gerd Von Rundstedt and Erwin Rommel into believing that Pas de Calais would be the main invasion site. Information warfare disrupted the Germans' decision--making process, primarily due to corrupted data.[6]

More recently during Operation Desert Storm, the coalition's information technology provided commanders with intelligence, flexibility, synchronization, and decision--making tools at a level beyond anything ever experienced in war. In this conflict, we clearly won the information war. The air campaign knocked out the Iraqi intelligence apparatus, which gave us sufficient cover to move two American corps and two allied divisions - one French

and one British - west, where they positioned themselves for the surprise ground attack. Likewise, information operations in the battlefield enabled commanders to communicate at unlimited distances, though there were problems when commanders were on the move. Our communications, command and control, computers, and intelligence networks allowed our battlefield commanders to dictate the tempo of operations and quickly bring lethal force on the enemy. The Desert Shield/Desert Storm campaign brought us into a new era of information warfare.

Now, winning the information war is an absolute must. The ability to collect and act on information quicker than your opponent is essential for winning on battlefields today and in the future. Now all leaders must be computer literate, with thorough independent knowledge of new information--based systems. I foresee a battlefield where interoperability barriers will be broken and satellite commuications will enable commanders to pass oral directives as easily as making a cellular telephone call today.

However, as the Department of Defense pursues these new technologies, we must anticipate vulnerabilities to information warfare. As information--based systems become more available, the vulnerabilities of these systems to corruption, attack, or disruption become more subtle, profuse, and challenging. Leaders and planners must be aware of these vulnerabilities.

THREATS TO INFORMATION--BASED SYSTEMS

Modern militaries are utterly dependent upon information technology to maintain, deploy, and employ virtually every weapon system in their arsenals[7]. By reducing uncertainity, information technology has become key to the decision-making process. Effective decision--making hinges on certainty and time: leaders prefer to wait as long as possible to gather and analyze the maximum amount of information before making a decision. Enhanced knowledge optimizes certainty, which in turn increases the probability of a good decision. On the other hand, lack of knowledge causes uncertainty, which increases the likelihood of a poor decision[8].

The Defense Information Systems Agency (DISA) says that hacker attacks on the Pentagon's global computer networks are detected twice daily. LTG Alonzo Short, then Director of DISA and VADM J.M. McConnell, National Security Agency Director, acknowledged in a 14 June 1994 letter that intruders have repeatedly and easily demonstrated the capability to penetrate and control various DoD computers used for finance, research and development, personnel, health, logistics and other support agencies[9]. Even though earlier generations of these systems were not sufficiently essential to threaten, by their disruption, the nation's ability to conduct war, they have now become the heart of the nation's ability to mobilize for war.

Our previous defense doctrine has been focused on protecting

America's shores, often with the assumption that the enemy would not have the capability or foolhardiness to invade the United States. As we enter the new paradigm of the information age, this insular, self--confident philosophy must change. Futurist Alvin Toffler offers a not too far--fetched example of information warfare: "We know a former senior intelligence official who says, 'Give me a billion dollars and 20 people and I'll shut America down. I'll shut down the Federal Reserve, all the ATMs [Automatic Teller Machine]; I'll desynchronize every computer in the country."

Further, as Paul A. Strassmann, Visiting Professor of Information Warfare at the National Defense University, points out, "Now, any two--bit dictator can invade us electronically and do great damage with virtually impunity." Not only is the U.S. ill-prepared for such attacks, but we currently lack the legal and policy framework for dealing with such intrusions. An adversary using counter--information warfare will not find it necessary to attack our combat forces, he will simply attack our information systems. Deputy Director of the CIA William O. Studeman has cited potential targets:

The morale and psyche of the U.S. public: "Subversion or denial of a service (telephone, television, computer networks) might be more effective-and cheaper-than destruction." FM 100-6 (Draft), Information Operations, cites this threat: "Misinterpretation,inaccurate information, misinformation (or disinformation) will impact upon families and communities, as

well as the soldiers; affecting their morale and commitment to the objective at hand, potentially undermining the critically important human psychological dimensions."

The information infrastructure: Power distribution, telephone and banking systems; systems of strategtically important companies; and high-tech databases[10].

It is no secret that the United States government (military and federal agencies) and civilians are ill--prepared to deal with threats imposed by information warfare. According to officials at the National Defense University, we need a full--scale review of information warfare. These officials recommend creation of a bipartisan commission with the clout to codify and fund a national response to the myriad ways potential enemy nations or terrorist groups could wreak incalculable havoc on the nation's exposed information infrastructure[11].

A not-too-sophisticated adversary could do some serious damage to this country. For example, the Federal Reserve System transfers about $1 trillion a day around the country, a process whose interruption could pose a threat to national security. However, exactly what sort of information--warfare acts pose the greatest security threats has yet to be defined. Most government agencies outside the Department of Defense have yet to focus on the danger[12].

Retired Vice Admiral Jerry Tuttle, vice president of Oracle Corporation, asserts that, "While the U.S. information infrastructure does have redundant systems that make it hard to

disrupt, terrorists and malevolent hackers could wreak havoc on U.S. society by knocking out key components, and protection against the complete destruction of the system is by no means assured[13]."

Information Warfare brings war--winning strategy into an entirely new battlespace. When any society "delegates decision making to the microchip," they create vulnerabilities within any center of gravity where the rapid manipulation of large quantities of information is critical. In future wars, a commander's first task may be to quickly gain and maintain information dominance and advantage, with the goal of getting inside the opponent's decision loop to mislead or deceive them[14].

Leaders and planners must be aware of the implications of information warfare. To counter the threats of information warfare, developers must determine whether (and how) friendly digitized systems can be crippled by a nonnuclear electromagnetic pulse, then they must design appropiate defenses. They must also determine physical constraints that the electromagnetic spectrum places on communications systems, then the information architecture should be built with these constraints in mind. Finally, planners must recognize that digitization may increase susceptibility to deception[15].

The Gulf War proved the value of information warfare when coalition forces destroyed the enemy's ability to conduct war. Accurate intelligence and the ability to pass that information

quickly allowed combat forces to strike quickly and decisively. This advantage produced a damaging effect on the decision--making ability of Iraqi leadership to conduct war. The ability to gain and act on information more quickly than your opponent is the foundation for winning on battlefields of today and the future. Through effective information warfare, we can cripple an enemy's decision-making ability.

On the other hand, the U.S. must take measures to protect our information--based systems. Constrained defense budgets and the U.S. government's snail--paced, arcane acquisition system virtually preclude in--house development of a cost--effective information warfare capability[16]. Therefore, our that government should work closely with civilian industry in the development of new security technology and efficient sytems to wage information war. Indeed civilian industry has equal reason to be concerned about information warfare. Security expert Arnaud de Borchgrave estimates that in just two months of 1995, about $300 million dollars has disappeared, electronically, from U.S. banks. High tech computer criminals now conduct crime internationally through the INTERNET.

Unfortunately, industry and government have not yet begun to cooperate extensively in securing our communication and data systems. The commerical sector has little tolerance for government--imposed restrictions, specifications, and acquisition rules. Companies can't be competitive in the marketplace if they have to move at government's pace, so they simply refuse to be

saddled by the many restrictions[17]. Therefore, government must change to keep pace with the commerical sector. We need an agency like DISA to serve as the single management agency for information warfare; representatives of private U.S. financial, industrial, and educational institutions should serve actively in this agency's role. In the meantime, the services must continue to pursue new information--based technologies and improve our wartime fighting capabilities.

INFORMATION OVERLOAD

Desert Shield/Desert Storm should have taught us a valuable lesson about the management of robust information--based systems. How do you manage information when existing technology can readily transfer all the information in the largest set of encyclopedias in seconds. In Earth in the Balance, Vice President Al Gore contends that "We now face a crisis entirely of our own making. We are drowning in information. We have generated more data, statistics, words, formulas, images, documents, and declarations than we can possible absorb. And rather than create new ways to understand and assimilate the information we already have, we simply create more information and at an increasingly rapid pace."

When I talk with Army officers of the various branches and officers of the sister services about their concerns with automation, they offer a common response: too much information. As the Chief, Data Networks Branch in the White House Communications Agency (WHCA) from 1983-1987, I recall that we integrated computers as our primary means of providing communications and office automation support to the President on trips away from the White House. There was an instant increase in the amount of information to be processed which necessitated the average support team to increase from 30 members to 50. In addition, the amount of support equipment grew to the point where a C-130 could no longer meet our transportation needs, only a C-

141. However, our initial objective in enhancing our technology was not only to provide a more efficient service but also to reduce our manpower. We definitely became more efficient, but we never achieved our manpower goals. As a matter of fact, by my departure in 1987 both the support teams from the WHCA and Presidential Staff had gotten larger. An overriding question remains; "Was all the additional information being provided really needed?"

General Frederick M. Franks, Jr. (Ret.), former commander of VII Corps, concurs, "As we generated more information to meet the more complex demands of modern warfare, staffs necessarily grew to a size that they could not be drug along with the commander to the fight. We need a new paradigm[18].

LTC Paul F Roques, Jr. makes the same point in his 1989 Army War College Military Studies Project: He observes that information overload can affect the weakest link-the chain of information processing. The great majority of analysts agree that information overload presents a fundamental problem. The knee--jerk solution to this problem has been to make staffs larger.

But information overload also impacts on the decision--making process of leaders. Colonel Charles T. Rogers of the British Army believes that the more information a commander has, the more reluctant the commander becomes to make decisions. There is a tendency either to become immobilized by information or to wait for yet another seemingly vital piece of information

that seems never to come. Rogers likens military leaders to prisoners of technology, in that analytical processes for sorting the information to determine what to use and how to use it themselves become very demanding of time and of information transmission and processing capabilities. He argues that analytical or scientific approaches to decision--making are better suited to training preparation, whereas the battlefield needs the "pull" based on intuition rather than the "staff push" of information[19].

Rogers further opines that for a commander to make appropriate intuitive decisions, he must be as far forward as possible. He should not remain at a command post where his clarity of vision will be impaired by confusing information." Even if the overload is really data overload resulting from improper filtering and processing, the commander nonetheless needs to strike a balance between too much and too little information, recognizing possible errors of omission and commission and the costs associated with each. The commander needs continued acess to a principal information agent who understands his intent and his decisional information requirements. The commander needs such means of quickly and effectively translating information into decisions and orders.

Carl W. Lickteig at Fort Knox, Kentucky, conducted research on information management by future platoon leaders. His findings highlight the impacts of information overload on the decision--making process of young leaders. Using participating

platoon leaders, Lickteig completed a series of information management exercises that systematically varied the number and revelance of messages received during a simulated delay-in-sector mission. Performance measures included information processing accuracy and speed and the type of actions resulting from messages received during each exercise. Additional measures included an objective measure of participants' awareness of the battlefield situations portrayed by the exercises and subjective measures of workload, situational awareness, and the relative contributions of voice versus digital communciations for selected command, control, and communication functions[20].

Lickteig's findings demonstrated that the amount of information and its relevance significantly affected the performance of participating platoon leaders using a future automated command and control system. In his evaluation, high information load resulted in reduced awareness of battlefield space and the loss of appropriate information conveyed to platoon leaders' superiors and subordinates. More specifically, high--volume participants were less accurate in their knowledge of reported enemy and friendly locations, and they passed fewer messages that should have been relayed. On the other hand, low--volume participants relayed too much information[21].

Lickteig discovered that information relevance had very pronounced effects on the platoon leaders' management of it. Less relevant information disrupted the flow of communication, caused inappropriate relays and impaired participants' ability to

accurately "see" their battlefield situation. More specifically, it took participants more time to read and relay low--relevance information, and its reception significantly reduced participants' relays of appropiate information. Low--relevance information also caused inappropriate relays to superiors and subordinates, and less accurate comprehension and projection of the platoon leader's battlefield situation[22].

Lickteig's results also indicated that vehicle--based commanders should selectively filter information they receive. By restricting relays to more appropriate messages, commanders can reduce the information load on their superiors and subordinates. Information relevance, determined by proximity, proved to be an important consideration in reducing the information management requirements of the platoon leader, his superiors and his subordinates[23].

All leaders must be aware of problems of information overload. To deal with this problem, leaders must request specific information or train their staffs to filter appropiate toward more defined objectives. This will allow for quick translation of data into knowledge and application. For example, if unspecified intelligence reports are requested, today's technology will provide the requestor with intelligence data concerning a specific area of operations, and the rest of the world as well. However, if information is requested for a specific area of operations, then information will be tailored for just that area, the staff can work it more efficiently.

Also, only a limited number of communication links will be available under a two multiple regional conflicts (MRC) strategy. We should always remember that information--based technologies are being developed to enhance the decision--making process, not to hinder or obfuscate it.

LEGAL CONSIDERATIONS OF INFORMATION WARFARE

Offensive information warfare consists of corrupting, destroying, or denying transmission of an adversary's data; defensive information warfare consists of protecting U.S. information--based systems. Technology provides many different ways to deny, corrupt, or destroy information--based systems. But what are the legal parameters for protecting a country from such intrusion--particularly when such security apparatus impacts the decision--making process of military, economic, and governmental decisions?

Needless to say, legal ramifications of information warfare raises some tough questions. For example, in an electronic environment, when does war begin? Before or after we make decisions on corrupted information? Does a malicious probe of a U.S. computer system warrant a quid pro quo response or a traditional combat response? Who decides to deploy offensive information weapons? Would a U.S. launched systems attack require Congressional approval? Is it legal to jam or scramble a commerical satellite signal to prevent the media from broadcasting an event real--time to the American people (a solution advocated by many of my War College classmates)?

Technology has clearly outpaced existing laws governing information-based communications. Admiral William O. Studeman, Deputy Director of the CIA, recently observed, "We need hacker prosecution laws, better definition of computer crime, and an

examination of the legal basis for appropiate government action in protecting information systems. Senator William Cohen (R-Maine) is presenting a bill in Congress to establish the position of Chief Information Officer (CIO) of the United States. Lobbyists are seeking to establish information security as primary CIO responsibility.

Legal aspects of information warfare must be quickly clarified due to our reliance on commerical and military information--based systems. Every day the decision--making processes of our nation's civilian and governmental leaders are critically dependent on information--based technologies capabilities to provide accurate, real--time, uncorrupted data. We need strong laws to govern the protection of these systems. The time has come to draw a line in cyberspace.

THE FUTURE

We have only begun to experience the technological wonders of information-based systems. In the United States, 622 million pieces of mail are posted daily; million of faxes are sent; tens of millions of electronic messages are sent over local networks; between 20 to 50 voice messages per adult are recorded daily; and the number of electronic mail (E-Mail) boxes will grow from 3.5 million to more than 40 million over the next 10 years[24]. Communciations systems in the near future will bring the battlefield picture from the foxhole to the Pentagon. Leaders and staffs will be challenged to quickly and effectively translate real-time information into effective decisions.

Effective decision--making hinges on certainty and time: leaders prefer to wait as long as possible to gather more information before making a decision. A commander who is able to reduce uncertainty in a timely fashion in any of the three areas of friendly force status, "enemy" force status, or the environment will make more effective in making decisions. Better decision--making ability enables a commander to effectively perform the functions of command and control: planning, directing, coordinating and controlling forces[25].

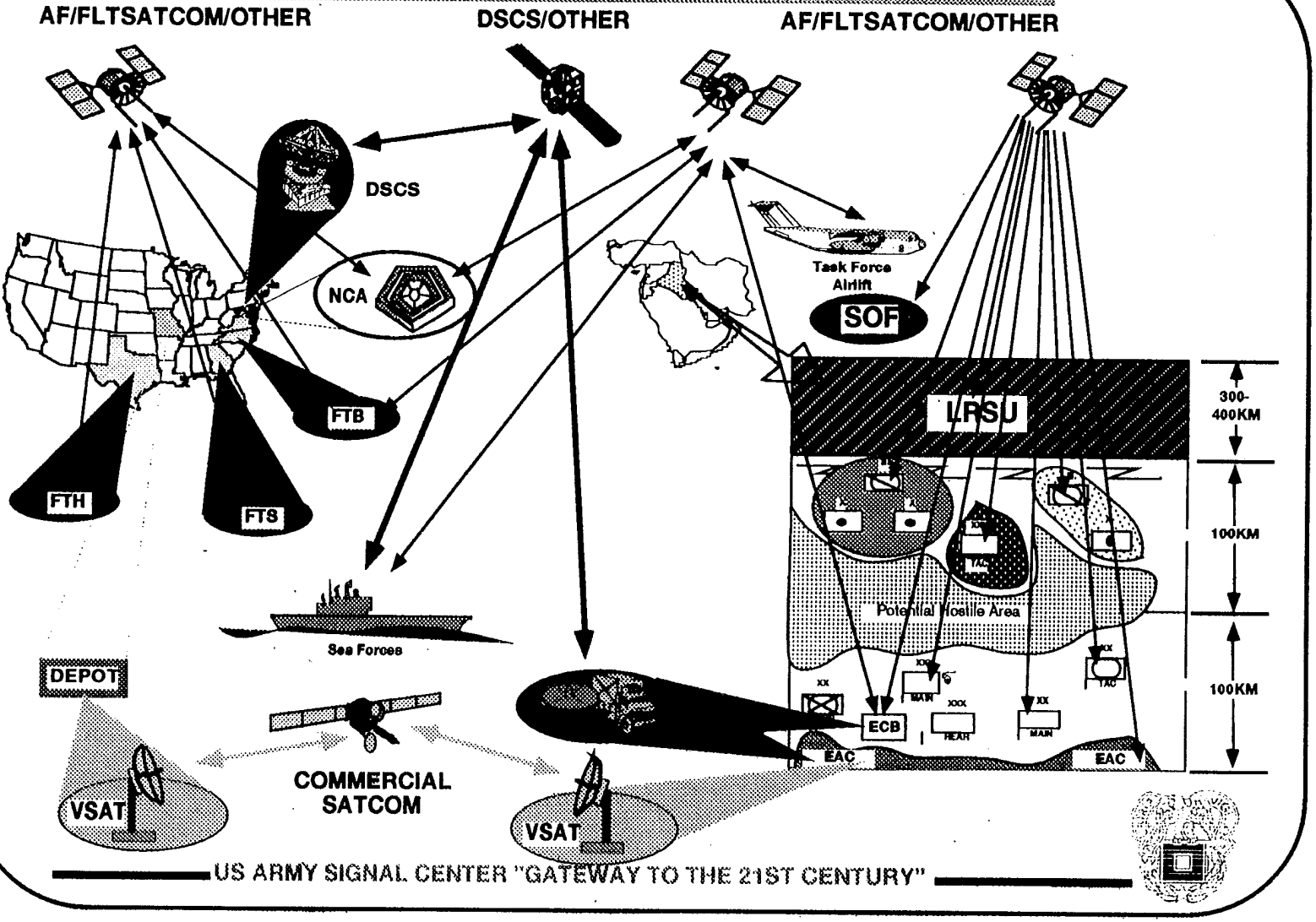
Good old American know--how will reduce future uncertainties. The Defense Department's Force XXI vision offers a very positive step. This plan revolves around the digitized battlefield. Digitization offers the commander added value

through integration of digital technologies across the breadth and depth of the battlefield. These digital technologies bring together computer microprocessor and memory chips with digital communciations systems, enabling us to store and transfer large amounts of information in a short time[26].

Digitization will reduce uncertainty through a more timely flow of an increased volume of information, which precisely informs commanders about the status of their own forces: location, maintenance status, activity, and personnel status. Similarly, more timely flow of an increased volume of information significantly reduces uncertainty about the status of enemy forces and the entire battlefield. Synergistically, digitization provides better information on which to base decisions; it gives the commander more time for making critical decisions[27].

The Department of Defense depends on space systems to move information over great distances and to respond quickly across the entire battlefield (see fig.1). The Department of Defense has projected that future satellite communications capacity requirements will increase by 50 per cent,from 1 billion bits/second in 1992 to 1.5 billion bits/second in 1997[28]. Economics will force the Pentagon to rely heavily on robust, commerically developed space systems and associated ground--based networks to conduct cost--effective information warfare. Space--based systems and battlefield digitization will reduce uncertainty, thus enhancing the decision--making process.

CURRENT SATCOM ARCHITECTURE



CONCLUSION

In President Clinton's recent State of the Union message, he urged that by the year 2000 computers and computer networks will be in every school in America. Microchip performance doubles every 18 months. Satellite broadcast systems have brought the media to anyone who can buy a satellite dish and receiver. My 11-year-old son, residing in Evans, GA., has a new checkers partner who is not the next door neighbor; he competes with another 11-year-old residing in New York City. They play checkers over the INTERNET. Yes, the information age has come home.

The United States has certainly not entered the information age alone. The world itself has been networked into this growing environment. Hostile governments and info--terrorists now have access to real--time, tactical reconnaissance for armies, cheap intelligence, and mass media propaganda systems. As we pursue information dominance, we must focus on protecting our information--based processes and information systems--as vital components of information dominance. Given the current vulnerabilities of our information-based systems, commanders must be fully prepared to make decisions in an operational environment of ambiquity, characterized by imperfect information and incomplete understanding of the situation. Command decision--making will remain an art, not a science, even in the Information Age.

Desert Shield/Desert Storm demonstrated the importance of

information dominance and the impacts on decision--making when leaders lose the capabilities to quickly gather information and make accurate decisions, a lesson Iraqi leadership will never forget. Are U.S. leaders prepared to operate against a technological foe possessing a similar capability to disrupt or corrupt our information--based systems?

Surley a lack of information hinders the overall effectiveness of the decision--making process. The most effective counter to information warfare on U.S. information--based systems is people. Highly trained and disciplined soldiers, civilians, and workers in industry. People are what got us in the information age, and properly trained people will enable us to survive even when the decision--making process of our leaders may be flawed. Soldiers, sailors, marines, airmen, and civil servants are our most important resource now. They will remain so in the future.

We must continue to pursue technologies which will advance our information-based systems. However, as the Department of Defense pursues these capabilities, vulnerabilities of information warfare must be recognized. Once any intruder gains access to a database, it can be corrupted. Imagine the implications for decision-making based on corrupted data: the results could be devastating. Achieving information dominance in a theater of war is an absolute. The ability to collect and act on information quicker than our opponent is essential for winning on battlefields today and in the future.

All leaders must be computer literate, with thorough independent knowledge of new information--based systems. Information--based terminology must be completely understood in order to confront the issues of vulnerabilities and threats to affective decision--making. Only the best soldiers and leaders will be successful in the information age. The American public expects quick and decisive victories. Emerging information technology gives our leadership the tools to meet this expectation and achieve decisive victory! Confronting the issues of information--based vulnerabilities will reduce threats on the decision--making process. We truly achieve information dominance, only when we have overcome such vulnerabilities. Cutting--edge technology offers us the advantage only so long as we prevent it from being cut apart at a critical time. We must maintain its security. We must have a fall--back resource when the security fails, for whatever reason.

ENDNOTES

1. Franks, Frederick M. Jr."Winning the Information War: Evolution and Revolution," Vital Speeches of the Day 60, 15 May 1994, 454.

2. Colonel Richard E. Riccardelli. "The Information and Intelligence Revolution." Military Review U.S. Army, Sep-Oct 1995: 82.

3. General Gordon R. Sullivan, U.S. Army, "Future Vision," Military Review, May-June 1995: 5.

4. Ibid., 5.

5. Ibid., 82; idem, The Information and Intelligence Revolution, 83.

6. Ibid., 83.

7. Ibid., 5; idem, Future Vision, 5.

8. Kurt C. Reitlinger, "Command and Control for Third Wave Warfare," ARMY, Vol:45 February 1995: 9.

9. June 14, 1994 letter through Emmett Paige, Jr., Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), to Deputy Defense Secretary John Deutch.

10. Anthes, Gary H. "New Laws Sought for Information Warfare." Computerworld Vol:29 Iss:23 June 5, 1995: 55.

11. Cooper, Pat, and Robert Holzer. "America Lacks reaction Plan for Info War." Defense News, No.10 (2-8 October 1995): 3.

12. Ibid., 3.

13. Ibid., 37.

14. Felker, Ed, Lt. Col., USAF, " A View of The Future," A Common Perspective, Joint Warfighting Center's Newsletter, Vol:3 No.2 September 1995: 17.

15. Ibid., 12; Command and Control for Third Wave Warfare, 12.

16. Scott, William B., "Information Warfare Demands New Approach," Aviation Week and Space Technology, March 13, 1995: 86.

17. Ibid., 88.

18. Ibid., 457; idem, Winning the Information War: Evolution and Revolution.

19. Laughridge, Gene. "Recent and Not-So Recent Thinking on Information Operations and the Knowledge War." Army Communicator 20 (Spring-Summer 1995): 34.

20. Lickteig, Carl W., "Information Management of Future Platoon Leaders: An Initial Investigation." U.S. Army Research Institute for the Behavorial and Social Sciences, June 1994, VII.

21. Ibid., 32.

22. Ibid., 33.

23. Ibid., 33.

24. Ibid., 85; idem, The Information and Intelligence Revolution.

25. Ibid., 9; idem, Command and Control for Third Wave Warfare, 9.

26. Ibid., 9.

27. Ibid., 10.

28. Williamson, John. "Winning the Data War." Jane's Defence Weekly Vol:23 No:20 May 20, 1995: 45.

BIBLIOGRAPHY

Anthes, Gary H."New Laws Sought for Information Warfare." Computerworld, 5 June 1995, 55.

Cooper,Pat,and Robert Holzer."America Lacks Reaction Plan for Info War." Defense News 10, 2-8 October 1995, 3,37.

Deutch, John, Deputy Secretary of Defense. Letter through Emmett Paige, Jr., Assistant Secretary of Defense for Command, Control, Communications and Intelligence (C3I), 14 June 1994.

Felker, Ed, Lt.Col., USAF."A View of the Future." A Common Perspective, Joint Warfighting Center's Newsletter 3, September 1995, 9-14.

Franks, Frederick M. Jr."Winning the Information War: Evolution and Revolution." Vital Speeches of the Day 60, Iss:15, 15 May 1994, 453-458.

Laughridge, Gene. "Recent and Not-So-Recent Thinking on Information Operations and the Knowledge War." Army Communicator 20, (Spring-Summer 1995): 32-38.

Lickteig, Carl W. "Information Management of Future Platoon Leaders: An Initial Investigation." U.S. Army Research Institute for the Behavioral and Social Sciences, June 1994, 1-79.

Reitlinger, Kurt C. "Command and Control for Third Wave Warfare." Army 45, February 1995, 9-14.

Riccardelli, Richard E., Colonel. "The Information and Intelligence Revolution." Military Review, May-June 1995, 4-14.

Scott, William B. "Information Warfare Demands New Approach." Aviation Week and Space Technology, 13 March 1995, 85-88.

Sullivan, Gordon R., General, U.S. Army. "Future Vision." Military Review, May-June 1995, 4-14.

Williamson, John. "Winning the Data War." Jane's Defence Weekly 23, 20 May 1995, 44-46.